Sous-groupes distingués et groupes quotients

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

Ce complément concerne principalement la leçon suivante :

103 Conjugaison dans un groupe. Exemples de sous-groupes distingués et de groupes quotients. Applications.

En particulier, je vous incite fortement à aller lire le passage du rapport du jury correspondant (et même le rapport en entier), qui fait presque une page !

1 Groupes quotients

1.1 Quotient par une relation d'équivalence

Soit E un ensemble muni d'une relation d'équivalence $\sim$.

Définition 1.1. L'ensemble *quotient* $E/\sim$ est l'ensemble des classes d'équivalences de E pour la relation $\sim$.

On peut voir $E/\sim$ comme un sous-ensemble de $\mathcal{P}(E)$. La surjection canonique $\pi : E \to E/\sim$ qui à un élément $x \in E$ associe sa classe d'équivalence $\overline{x}$ vérifie $\overline{x} = \overline{y} \iff x \sim y$.

1.2 Quotient par un sous-groupe

Soit G un groupe et H un sous-groupe. On considère la relation d'équivalence $\sim$ sur G donnée par $x \sim y$ si $x^{-1}y \in H$. La classe d'équivalence d'un élément $x \in G$ est xH. L'ensemble quotient, noté G/H, est appelé ensemble des *classes à gauches*. On peut de même définir les *classes à droite* $H\backslash G$, obtenues comme classes d'équivalences pour la relation $x \sim' y \iff xy^{-1} \in H$.

Remarque 1.2. Si G est abélien alors les notions de classe à gauche et à droite coïncident. En général, ce sont deux notions différentes. On va voir une CNS sur H pour que ces deux notions coïncident.

Remarque 1.3. Dans tous les cas, les ensembles G/H et $H\backslash G$ sont toujours en bijection. En effet, l'application $x \mapsto x^{-1}$ envoie une classe à gauche xH sur la classe à droite Hx^{-1}.

2 Sous-groupe distingué

Soit G un groupe et H un sous-groupe. Il est naturel de voir si on peut munir G/H d'une structure de groupe telle que la surjection canonique $\pi : G \to G/H$ (donnée par $\pi(x) = xH$) est un morphisme de groupes. Remarquons que π est un morphisme de groupe ssi pour tout $x, y \in G$ on a $\overline{xy} = \overline{x} \cdot \overline{y}$, en d'autres termes ssi la loi sur G/H est compatible avec celle sur G.

Proposition 2.1. *L'application π est un morphisme de groupes ssi $xH = Hx$ (i.e. $xHx^{-1} = H$) pour tout $x \in G$.*

Démonstration. Soit $x \in G$. Par hypothèse on a $\pi(x) = \pi(1)\pi(x)$ donc $xH = HxH$ donc $xH \supseteq Hx$ (puisque $1 \in H$). L'inclusion $Hx \subseteq xH$ étant valable pour tout $x \in G$, on a également $Hx^{-1} \subseteq x^{-1}H$ donc $xH \subseteq Hx$ et donc $xH = Hx$. On conclut que $xHx^{-1} = H$ puisque les translations sont des bijections.

Réciproquement, on a $\pi(xy) = xyH = xyHH = xHyH = \pi(x)\pi(y)$ donc π est bien un morphisme. □

Définition 2.2. Si le sous-groupe H vérifie la condition précédente :

$$xHx^{-1} = H, \qquad \text{pour tout } x \in G,$$

on dit que H est un sous-groupe *distingué* de G et on note $H \triangleleft G$.

Comme on a vu dans la preuve de la Proposition 2.1, un sous-groupe H est distingué dans G ssi

$$xHx^{-1} \subseteq H, \qquad \text{pour tout } x \in G.$$

Remarque 2.3. Soit x tel que $xHx^{-1} \subseteq H$. Si H est fini alors puisque les translations sont des bijections on a $|xHx^{-1}| = |xH| = |H|$ donc $xHx^{-1} = H$. Si H est infini, comme on l'a vu si l'inclusion $x^{-1}Hx \subseteq H$ est également vraie alors $xHx^{-1} = H$. En général, on n'a pas égalité, comme le montre l'exemple suivant. Dans le groupe $\mathrm{GL}_2(\mathbb{Q})$, on considère le sous-ensemble

$$G_\alpha := \left\{ \begin{pmatrix} \alpha^n & k \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}, k \in \mathbb{Q} \right\},$$

pour $\alpha \in \mathbb{N}_{\geq 2}$ donné. Avec la relation

$$\begin{pmatrix} \alpha^n & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^m & l \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha^{n+m} & l\alpha^m + k \\ 0 & 1 \end{pmatrix}, \tag{2.4}$$

on vérifie que G_α est bien un (sous-)groupe. On regarde maintenant

$$H_\alpha := \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix},$$

qui est bien un sous-groupe de G_α, toujours par (2.4) (et par ailleurs $H_\alpha \simeq \mathbb{Z}$). L'élément

$$g := \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix},$$

vérifie, pour $k \in \mathbb{Z}$,

$$g \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} \alpha & \alpha k \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} \alpha & \alpha k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha k \\ 0 & 1 \end{pmatrix} \in H_\alpha,$$

puisque $\alpha, k \in \mathbb{Z}$, donc $gH_\alpha g^{-1} \subseteq H_\alpha$. En revanche, toujours pour $k \in \mathbb{Z}$ on a

$$g^{-1} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} g = g^{-1} \begin{pmatrix} \alpha & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^{-1}k \\ 0 & 1 \end{pmatrix}.$$

En prenant par exemple k tel que $0 < k < \alpha$, ce qui est possible puisque $\alpha \geq 2$, on en déduit que $g^{-1}H_\alpha g \not\subseteq H_\alpha$.

(En fait (2.4) montre que G_α est isomorphe à un produit semi-direct $\mathbb{Z} \ltimes \mathbb{Q}$, le sous-groupe H_α est l'image de $(0, \mathbb{Z})$ et g est l'image de $(1, 0)$.)

Dans certains énoncés, si on a besoin qu'un sous-groupe H soit distingué dans G on peut remplacer G par le *normalisateur*

$$\mathrm{N}_G(H) \coloneqq \{x \in G : xHx^{-1} = H\}.$$

de H dans G. C'est un sous-groupe de G qui contient H dans lequel H est distingué.

Remarque 2.5. On peut également considérer le pseudo-normalisateur $\{x \in G : xHx^{-1} \subseteq H\}$. Il coïncide avec le normalisateur quand H est fini mais n'est en général pas un sous-groupe de G (voir la Remarque 2.3).

Propriété 2.6. *Un sous-groupe distingué est une union (disjointe) de classes de conjugaisons.*

Attention, une union de classes de conjugaisons n'est pas nécessairement un sous-groupe !

Proposition 2.7. *Soit H un sous-groupe distingué de G. La surjection canonique $\pi : G \to G/H$ induit une application bijective*

$$\tilde{\pi} : \begin{array}{ccc} \{\textit{sous-groupes de } G \textit{ contenant } H\} & \overset{1:1}{\longleftrightarrow} & \{\textit{sous-groupes de } G/H\} \\ K & \longmapsto & \pi(K) = K/H \end{array},$$

d'inverse $\pi^{-1}(\overline{K}) \hookleftarrow \overline{K}$. L'énoncé reste vrai si l'on se restreint (des deux côtés) aux sous-groupes distingués.

Démonstration. Exercice. Remarquons que si $H \subseteq K \triangleleft G$ alors pour montrer que $\pi(K) \triangleleft G/H$ on utilise que π est surjective. De plus, pour montrer que l'inverse de $\tilde{\pi}$ est bien l'application annoncée, on dit (dans un sens) que $x \in \pi^{-1}(\pi(K)) \iff \pi(x) \in \pi(K) \iff x = kh$ donc $x \in K$, ainsi $\pi^{-1} \circ \pi(K) \subseteq K$ et l'autre inclusion est vérifiée par définition de π^{-1}. □

Exemple 2.8. Les sous-groupes propres non triviaux de $\mathbb{Z}/6\mathbb{Z}$ sont $2\mathbb{Z}/6\mathbb{Z}$ et $3\mathbb{Z}/6\mathbb{Z}$.

Si $H, K \leq G$, on note $HK \coloneqq \{hk : h \in H, k \in K\}$.

Proposition 2.9. *Soient H et K deux sous-groupes de G.*
- *Si $H \subseteq \mathrm{N}_G(K)$ ou si $K \subseteq \mathrm{N}_G(H)$ (en particulier, si H ou K est distingué dans G) alors $HK = KH$ est un sous-groupe de G.*
- *Si H et K sont distingués dans G alors HK est un sous-groupe distingué de G.*
- *Si H et K sont distingués dans G et si $H \cap K = \{1\}$ alors $HK \simeq H \times K$.*

Remarque 2.10. Si H ou K est distingué dans G et si $H \cap K = \{1\}$ alors HK est isomorphe à un produit semi-direct entre H et K. (La notion de produit semi-direct est dans la limite extérieure du programme de l'agrégation.)

Remarque 2.11. Revenons à la Proposition 2.7. Si K est un sous-groupe quelconque de G alors $\pi(K)$ est encore un sous-groupe de G/H mais cependant

$$\pi^{-1}(\pi(K)) = KH.$$

En effet, si $x \in \pi^{-1} \circ \pi(K)$ alors $\pi(x) \in \pi(K)$ donc $\pi(x) = \pi(k)$ donc $x = kh$. Réciproquement, on a $\pi(kh) = khH = kH = \pi(k)$.

Concluons cette section par cette phrase de savoir-vivre mathématique : lorsque l'on a un sous-groupe distingué, il est bon d'identifier le quotient.

3 Exemples généraux

3.1 Exemples génériques

Soit G un groupe. On a déjà mentionné le résultat suivant.

Proposition 3.1. *Si G est un groupe abélien alors tous ses sous-groupes sont distingués.*

La notion de sous-groupe distingué n'apporte donc rien ici, mais les quotients n'en sont pas moins intéressants ; nous donnons ci-dessous quelques exemples.

- Pas besoin de préciser que $\mathbb{Z}/n\mathbb{Z}$ est très utilisé (arithmétique, corps finis premiers, cryptographie,...).
- Si k est un corps et $P \in k[X]$ est un polyôme irréductible alors $k[X]/(P)$ est un corps de degré $\deg P$ sur k (construction des corps finis, construction de $\mathbb{C}$, extensions de $\mathbb{Q}$,...).
- Le discriminant d'une formes quadratique non dégénérées sur un corps k peut se voir comme un élément de $k^*/(k^*)^2$ (le discriminant étant alors donné par le déterminant d'une matrice).
- L'espace des fonctions 1-périodique $\mathbb{R} \to \mathbb{R}$ peut se voir comme l'espace des fonctions de $\mathbb{R}/\mathbb{Z}$ (le « tore ») vers $\mathbb{R}$.
- Soit $f : E \to \mathbb{K}$ une forme linéaire d'un espace vectoriel normé E. Alors f est continue ssi $\ker f$ est fermé. En effet, le sens direct est vrai (conséquence de la définition de la continuité), et si $\ker f$ est fermé alors $E/\ker f$ est de dimension 1. Ainsi, la forme linéaire f est une composition $E \to E/\ker f \to \mathbb{K}$ d'applications continues donc f est continue. En effet, la projection canonique $E \to E/F$ est toujours continue si F est un sev fermé (ce qui est le cas car $F = \ker f$ est fermé par hypothèse), et $E/\ker f$ est de dimension finie donc $E/\ker f \to \mathbb{K}$ est continue.
- Un *ensemble de Vitali*[1] est sous-ensemble V de l'intervalle $[0,1]$ qui contient exactement un représentant de chaque classe d'équivalence de $\mathbb{R}/\mathbb{Q}$ (attention, la construction d'une telle partie nécessite l'axiome du choix). C'est une partie non mesurable de $\mathbb{R}$ pour la mesure de Lebesgue : en effet, si elle était mesurable alors l'ensemble

$$W \coloneqq \bigsqcup_{\substack{r\in\mathbb{Q}\\ -1\le r\le 1}} (V + r) \subseteq [-1, 2],$$

  serait mesurable et V serait donc de mesure nulle. C'est une absurdité puisque W contient $[0,1]$, puisque tout élément $x \in [0,1]$ possède un représentant y dans V, donc $r \coloneqq x - y \in \mathbb{Q}$ et $r \in [-1,1]$ puisque $x, y \in [0,1]$.

Remarque 3.2. Attention, un groupe dont tous les sous-groupes propres sont distingués (un tel groupe est appelé *hamiltonien*) n'est pas nécessairement abélien. Pour cela, il suffit de regarder parmi les petits sous-groupes non abéliens. En ordre 6 ça ne va pas fonctionner puisque dans $\mathfrak{S}_3$ car $\langle(12)\rangle$ n'est pas distingué (car (12) et (13) sont conjuguées par exemple). En ordre 8, le groupe diédral $\mathbb{D}_4 = \langle r, s : r^4, s^2, (sr)^2\rangle$ (d'ordre 8) ne fonctionne pas car s est d'ordre 2 mais $rsr^{-1} = r^2 s \neq s$ donc $\langle s\rangle$ n'est pas distingué. En revanche, le groupe

$$Q = \langle i, j, k : (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1\rangle = \{\pm 1, \pm i, \pm j, \pm k\}$$

des quaternions convient. En effet, tout sous-groupe de cardinal 4 est distingué (car d'indice 2, cf. plus tard), et le seul sous-groupe de cardinal 2 est $\langle -1\rangle$ car -1 est le seul élément d'ordre 2 donc $\langle -1\rangle$ est nécessairement distingué (car tout conjugué est de même cardinal).

1. Giuseppe Vitali, italien, 1875–1932.

Définition 3.3. Un sous-groupe H de G est dit *caractéristique* si H est (globalement) stable par tout automorphisme de G.

Propriété 3.4. *Un sous-groupe caractéristique est distingué.*

Démonstration. Un élément $x \in G$ induit l'automorphisme (dit *intérieur*) donné par $\gamma_x : y \mapsto xyx^{-1}$. (Attention, avec $x^{-1}yx$ on obtient seulement un anti-morphisme.) □

Remarque 3.5. On a donc une application $\gamma : G \to \mathrm{Int}(G)$. Cette application est elle-même un morphisme, c'est-à-dire $\gamma_{xy} = \gamma_x \circ \gamma_y$.

Proposition 3.6. *Soit $K \subseteq H \subseteq G$ avec K caractéristique dans H. Si H est caractéristique (resp. distingué) dans G alors K également.*

Démonstration. On suppose d'abord H caractéristique dans G. Soit α un automorphisme de G. Par hypothèse, le sous-groupe H est stable par α donc α se restreint en un automorphisme α_H de H, sous lequel K est stable par hypothèse. On conclut puisque la restriction de α_H à K est la même que la restriction de α à K. Si maintenant H est distingué dans G, il suffit de prendre pour α un automorphisme intérieur. □

Remarque 3.7. L'énoncé précédent devient faux en général si l'on remplace « K caractéristique dans H » par « distingué dans H » (avec H distingué dans G). Par exemple, dans le groupe diédral $\mathbb{D}_4 = \langle r, s\rangle$ d'ordre 8, on a la suite $\langle s\rangle \triangleleft \langle s, r^2\rangle \triangleleft \mathbb{D}_4$ mais $\langle s\rangle$ n'est pas distingué dans $\mathbb{D}_4$ (par exemple car $rsr^{-1} \neq s$ car $rs \neq sr$ car $sr = r^{-1}s$ et $r \neq r^{-1}$ car r est d'ordre 4). Noter que $\langle s, r^2\rangle = \{1, s, r^2, r^2s = sr^2\} \simeq (\mathbb{Z}/2\mathbb{Z})^2$, en particulier $\langle s, r^2\rangle$ est d'indice 2 dans $\mathbb{D}_4$ donc est distingué et même chose pour $\langle s\rangle$ dans $\langle s, r^2\rangle$. (Attention, on ne peut pas remplacer $\langle s\rangle$ par $\langle r^2\rangle$ car ce dernier est distingué dans $\mathbb{D}_4$!) Avec un ordre plus grand mais le même type de contre-exemple, on peut prendre $\langle (12)(34)\rangle \triangleleft V \triangleleft \mathfrak{S}_4$.

Proposition 3.8. *Le* centre *de G*

$$\mathrm{Z}(G) = \{x \in G : xy = yx \text{ pour tout } y \in G\},$$

et son groupe dérivé

$$\mathrm{D}(G) = \big\langle [x, y] : x, y \in G\big\rangle,$$

*où $[x, y] \coloneqq xyx^{-1}y^{-1}$ (*commutateur*), sont des sous-groupes caractéristiques de G.*

Démonstration. Soit $\alpha \in \mathrm{Aut}(G)$. Si $x \in \mathrm{Z}(G)$ alors pour tout $y \in G$, on peut écrire $y = \alpha(z)$ et on a $\alpha(x)y = \alpha(x)\alpha(z) = \alpha(xz) = \alpha(zx) = \alpha(z)\alpha(x) = y\alpha(x)$ donc $\alpha(x) \in \mathrm{Z}(G)$. Pour le groupe dérivé c'est encore plus simple : pour tout $x, y \in G$ on a $\alpha\big([x, y]\big) = \alpha(xyx^{-1}y^{-1}) = \alpha(x)\alpha(y)\alpha(x)^{-1}\alpha(y)^{-1} = [\alpha(x), \alpha(y)] \in \mathrm{D}(G)$. □

Remarque 3.9. On a en fait montré que si $f : G \to H$ est un morphisme alors $f\big(\mathrm{D}(G)\big) \subseteq \mathrm{D}(H)$ et si de plus f est surjectif alors $f\big(\mathrm{Z}(G)\big) \subseteq \mathrm{Z}(H)$.

Le groupe G est abélien ssi $\mathrm{Z}(G) = G$ ssi $\mathrm{D}(G) = \{1\}$. Attention à ne pas dire que le groupe dérivé est l'ensemble des commutateurs (mais c'est faux à partir de l'ordre 96 seulement !). On applique maintenant l'adage précédent « qui dit trouve le sous-groupe distingué dit identifie le quotient ». Il faut connaître les centres et les groupes dérivés des groupes classiques (notamment $\mathfrak{S}_n$ et GL_n).

Remarque 3.10. (Suite de la Remarque 3.5.) Le noyau du morphisme $\gamma : G \to \mathrm{Int}(G)$ est $\mathrm{Z}(G)$. En effet,

$$\begin{aligned} x \in \ker\gamma &\iff \gamma_x = \mathrm{id}_G \\ &\iff \gamma_x(y) = y, \quad \text{pour tout } y \in G, \\ &\iff xyx^{-1} = y, \quad \text{pour tout } y \in G, \\ &\iff x \in \mathrm{Z}(G). \end{aligned}$$

On obtient donc l'isomorphisme $G/\mathrm{Z}(G) \simeq \mathrm{Int}(G)$.

Remarque 3.11. Le groupe $G/\mathrm{D}(G)$ est abélien, on a même la propriété suivante : si H est un sous-groupe distingué de G alors

$$G/H \text{ est abélien} \iff H \supseteq \mathrm{D}(G), \tag{3.12}$$

en d'autres termes, le groupe dérivé est le plus petit sous-groupe distingué de G tel que le quotient soit abélien de G. Le quotient $G^{\mathrm{ab}} \coloneqq G/\mathrm{D}(G)$ est appelé l'*abélianisé* de G.

Montrons maintenant l'équivalence ci-dessus. On a

$$\begin{aligned} G/H \text{ abélien} &\iff \overline{[x,y]} = 1, \quad \text{pour tout } x, y \in G \\ &\iff [x,y] \in H, \quad \text{pour tout } x, y \in G \\ &\iff \mathrm{D}(G) \subseteq H. \end{aligned}$$

On définit par récurrence la suite dérivée $\left(\mathrm{D}^i(G)\right)_{i\geq 0}$ de G par $\mathrm{D}^0(G) \coloneqq G$ et $\mathrm{D}^{i+1}(G) \coloneqq \mathrm{D}(\mathrm{D}^i(G))$.

Corollaire 3.13. *Le sous-groupe $\mathrm{D}^i(G)$ est un sous-groupe caractéristique de G pour tout $i \geq 0$.*

Démonstration. On a la chaîne de sous-groupes caractéristiques $\mathrm{D}^i(G) \subseteq \mathrm{D}^{i-1}(G) \subseteq \cdots \subseteq \mathrm{D}(G) \subseteq G$ et on conclut par la Proposition 3.6. □

On reparlera de cette chaîne de sous-groupes dans la Section 6.

3.2 Théorèmes d'isomorphismes

Commençons par la propriété universelle du quotient, qui permet de construire des morphismes.

Théorème 3.14 (Propriété universelle du quotient de groupes)**.** *Soit $f : G \to H$ un morphisme de groupes et soit $\ker f \supseteq K \triangleleft G$. Alors f se factorise de façon unique en un morphisme $\overline{f} : G/K \to H$, factorise au sens où $f = \overline{f} \circ \pi$ où $\pi : G \to G/K$ est la surjection canonique.*

Démonstration. Par hypothèse, le morphisme f est constant sur les classes à gauches pour K donc on a une application bien définie $\overline{f} : G/K \to H$ qui factorise f. C'est bien un morphisme car $\overline{f}(\pi(x)\pi(y)) = \overline{f}(\pi(xy)) = f(xy) = f(x)f(y) = \overline{f}(\pi(x))\overline{f}(\pi(y))$. □

On peut quotienter par $K \subseteq \ker f$ sans changer la valeur de f car « les éléments tués par le quotient le sont déjà par f ».

Application 3.15. Si $f : G \to H$ est un morphisme de groupes avec H abélien alors $\mathrm{D}(G) \subseteq \ker f$ et donc f se factorise en un morphisme $G/\mathrm{D}(G) \to H$. Par exemple, avec $G = \mathfrak{S}_n$ on obtient la factorisation $\mathfrak{S}_n \to \mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z} \to H$. Ainsi, si H ne possède pas d'élément d'ordre 2 alors f est trivial, et sinon $f = f_h$ est de la forme $f_h(\sigma) = \begin{cases} 1, & \text{si } \epsilon(\sigma) = 1, \\ h, & \text{sinon} \end{cases}$, où $h \in H$ est d'ordre 2.

Lemme 3.16. *Soit G un groupe et H un sous-groupe. Alors H est distingué dans G ssi il existe un groupe K et un morphisme $f : G \to K$ tel que $H = \ker f$.*

Démonstration. Le noyau est distingué car f est un morphisme, et si $H \triangleleft G$ alors H est le noyau de la surjection canonique $G \to G/H$. □

Remarque 3.17. On a le résultat suivant (voir F. Ulmer, *Théorie des groupes*, §17.3 ou G. Peyré, *L'algèbre discrète de la transformée de Fourier*, §VIII.1.3). Soit G un groupe fini et $\chi_1, \dots, \chi_m$ ses caractères irréductibles. Tout sous-groupe distingué de G est de la forme $\cap_{j\in J} \ker \chi_j$ pour J décrivant les sous-ensembles de $\{1, \dots, m\}$, avec la notation $\ker \chi = \{g \in G : \chi(g) = \chi(1)\}$. On peut ainsi déterminer les sous-groupes distingués à partir de la table de caractères du groupe.

Théorème 3.18 (Premier théorème d'isomorphisme)**.** *Si $f : G \to H$ est un morphisme de groupes alors f induit un isomorphisme $G/\ker f \simeq \operatorname{im} f$.*

Démonstration. Découle des deux résultats précédents. En particulier, le noyau du morphisme induit $\overline{f} : G/\ker f \to \operatorname{im} f$ est bien trivial puisque $\overline{f}(\pi(x)) = 1 \iff f(x) = 1 \iff x \in \ker f \iff \pi(x) = 1$. □

On donnera une multitude d'application dans la Section 4, sans compter les deux théorème suivants.

Théorème 3.19 (Deuxième théorème d'isomorphisme)**.** *Soit G un groupe et N, H deux sous-groupes avec $H \subseteq \mathrm{N}_G(N)$ (c'est en particulier le cas quand $N \triangleleft G$). Alors $H \cap N$ est distingué dans H et $HN/N \simeq H/(H \cap N)$.*

Démonstration. L'application canonique $f : H \to HN/N$ est surjective puisque $hnN = hN = f(h)$. Pour $h \in H$, on a $h \in \ker f \iff h \in N$ donc $\ker f = H \cap N$ et on conclut par le premier théorème d'isomorphisme. □

Théorème 3.20 (Troisième théorème d'isomorphisme)**.** *Soient $M \subseteq N$ deux sous-groupes distingués de G. Alors (M est distingué dans N et) N/M est un sous-groupe distingué de G/M et*

$$(G/M)/(N/M) \simeq G/N.$$

Démonstration. Par le théorème de correspondance on sait que N/M est bien un sous-groupe distingué de G/M (puisque $N \supseteq M$ est un sous-groupe distingué de G ; remarquer qu'on n'utilise pas l'hypothèse $M \triangleleft G$ ici). Soit maintenant $f : G \to (G/M)/(N/M)$ le morphisme naturel. On a des flèches surjectives $G \xrightarrow{m} G/M \xrightarrow{n} (G/M)/(N/M)$ donc f est surjective. Si $x \in \ker f$ alors $m(x) \in \ker n$ donc $m(x) \in N/M$ donc $x \in N$ par le théorème de correspondance des sous-groupes. On conclut par le premier théorème d'isomorphisme. □

Remarque 3.21. Attention, le quotient $(G/M)/(G/N)$ n'a pas de sens à priori car G/N ne s'identifie pas naturellement à un sous-groupe (distingué) de G/M.

Application 3.22. L'abélianisé $G^{\mathrm{ab}} = G/\mathrm{D}(G)$ est le plus grand quotient abélien de G, au sens où si $H \triangleleft G$ avec G/H abélien alors G/H est un quotient de $G/\mathrm{D}(G)$. En effet, puisque G/H est abélien on a $H \supseteq \mathrm{D}(G)$ par (3.12), donc par le troisième théorème d'isomorphisme on a

$$G/\mathrm{D}(G)\Big/H/\mathrm{D}(G) \simeq G/H.$$

Dans les deux preuves ci-dessus, on voit bien qu'à chaque fois pour construire l'isomorphisme on est parti d'un morphisme très simple à définir et on utilise ensuite la définition du quotient et le premier théorème d'isomorphisme pour construire d'autres morphismes à partir de celui-là.

3.3 Quelques conditions suffisantes

Soit G un groupe. L'*indice* d'un sous-groupe est le cardinal du (pas nécessairement groupe) quotient.

Proposition 3.23. *Tout sous-groupe d'indice 2 est distingué.*

Démonstration. Si H est d'indice 2 et $x \notin H$ alors $G = H \sqcup xH = H \sqcup Hx$ donc $xH = Hx$ et H et distingué. □

Plus généralement, on a le résultat suivant.

Proposition 3.24. *On suppose que G est fini. Tout sous-groupe d'indice le plus petit facteur premier de $|G|$ est distingué.*

Démonstration. Soit p ce plus petit facteur premier et soit H un tel sous-groupe. Si H est trivial le résultat est vérifié, on suppose donc $H \neq \{1\}$. Le groupe H agit sur G/H par translation à gauche par $h \cdot gH = hgH$. On a $p = \sum_{\omega \text{ orbite}} |\omega|$, et puisque la classe H est stable par H, on en déduit que les orbites sont de taille au plus $p-1$. On a $p|H| = |G|$ et p est le plus petit facteur premier de G donc puisque $|H| \neq 1$ on en déduit que tous les facteurs premiers de H sont $\geq p$. On a vu que les orbites sont de taille au plus $p-1$ donc par la relation orbite-stabilisateur on en déduit que toutes les orbites sont de taille 1.

Ainsi, pour tout $h \in H$ et $g \in G$ on a $hgH = gH$ donc $g^{-1}hgH = H$ donc $g^{-1}hg \in H$, donc H est distingué dans G. □

Remarque 3.25. Ce théorème n'est pas facile à illustrer pour $p > 2$ les groupes non abéliens d'ordre impair ne sont pas simples à décrire. Pour information, les plus petits ordres de tels groupes sont 21, 27, 39, 55, 57, 63, 75, 81, 105, 111 (voir `A060652` sur l'OEIS).

On termine cette section avec une application des théorèmes de Sylow (hors programme, voir le Perrin pour plus d'informations)

Proposition 3.26. *Soit G un groupe d'ordre $p^\alpha m$ avec p premier et $p \nmid m$. L'ensemble des sous-groupes de G d'ordre p^α est de cardinal $n_p > 0$ avec $n_p \equiv 1 \pmod p$ et $n_p \mid m$. De plus G opère transitivement sur ces sous-groupes, en particulier si $n_p = 1$ alors l'unique sous-groupe d'ordre p^α est distingué.*

Ce théorème est particulièrement pratique pour classifier les groupes. On ébauche une application dans l'exemple suivant.

Exemple 3.27. Soient $p < q$ deux nombres premiers et soit G un groupe d'ordre pq. On a $n_q \equiv 1 \pmod q$ et $n_q \mid p$ donc $n_q = 1$. Ainsi G possède un unique sous-groupe d'ordre q, qui est distingué. (On peut montrer ensuite que si $p \mid q-1$ alors G est cyclique, et sinon G est soit cyclique soit non abélien (unique à isomorphisme près).)

4 Exemples classiques

Proposition 4.1 (Groupe symétrique)**.** *Le groupe alterné $\mathfrak{A}_n = \ker \epsilon$ est un sous-groupe distingué dans $\mathfrak{S}_n$ et c'est l'unique sous-groupe d'indice 2 de $\mathfrak{S}_n$. On a $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$.*

Proposition 4.2 (Groupe linéaire)**.** — *Le groupe spécial linéaire $\mathrm{SL}_n(k) = \ker \det$ est distingué dans $\mathrm{GL}_n(k)$ et $\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \simeq k^\times$.*

— *Le quotient de* $\mathrm{GL}_n(k)$ *(resp.* $\mathrm{SL}_n(k)$*) par son centre* $k^\times I_n$ *(resp.* $\mu_n(k)I_n$*) est le groupe projectif linéaire (resp. spécial linaire)* $\mathrm{PGL}_n(k)$ *(resp.* $\mathrm{PSL}_n(k)$*). Ces quotients agissent fidèlement sur l'ensemble des droites vectorielles de* k^{n+1} *(c'est* $\mathbb{P}^n(k)$*, l'espace projectif de dimension* n *sur* k*).*
— *Le groupe* $\mathrm{PSL}_n(k)$ *s'identifie à un sous-groupe distingué de* $\mathrm{PGL}_n(k)$ *et* $\mathrm{PGL}_n(k)/\mathrm{PSL}_n(k) \simeq k^\times/k^{\times n}$*, où* $k^{\times n} \coloneqq \{\lambda^n : \lambda \in k^\times\}$.

Démonstration. — On utilise $\det : \mathrm{GL}_n(k) \twoheadrightarrow k^\times$ qui est de noyau $\mathrm{SL}_n(k)$ et le premier théorème d'isomorphisme.
— Pour montrer l'assertion sur le centre il suffit d'utiliser les matrices de transvection (matrice identité + un coefficient non diagonal). Pour l'action sur les droites vectorielles, une matrice inversible stabilise toutes les droites ssi c'est une homothétie donc en quotientant par les homothéties on obtient bien une action fidèle.
— On veut montrer qu'il existe une injection $\mathrm{PSL}_n(k) \hookrightarrow \mathrm{PGL}_n(k)$. Pour cela, on regarde l'application canonique $\pi : \mathrm{SL}_n(k) \to \mathrm{PGL}_n(k)$. Si $M \in \ker\pi$ alors $M = \lambda I_n$ pour $\lambda \in k^\times$. Puisque $M \in \mathrm{SL}_n(k)$, on en déduit que $\lambda \in \mu_n(k)$ et donc $\ker\pi \subseteq \mu_n(k)I_n$. Réciproquement, si $M = \lambda I_n$ pour $\lambda \in \mu_n(k)$ alors $M \in k^\times I_n$ donc l'image de M dans $\mathrm{PGL}_n(k)$ est triviale. Ainsi, on a $\ker\pi = \mu_n(k)$ et π se factorise en l'injection $\mathrm{PSL}_n(k) \hookrightarrow \mathrm{PGL}_n(k)$ recherchée, notée $\overline{\pi}$.
Pour étudier le quotient, on regarde tout d'abord $d : \mathrm{GL}_n(k) \twoheadrightarrow k^\times/k^{\times n}$ donnée par le déterminant. On a $\ker d \supseteq k^\times I_n$ donc d se factorise via $\overline{d} : \mathrm{PGL}_n(k) \twoheadrightarrow k^\times/k^{\times n}$. Soit $M \in \mathrm{GL}_n(k)$ telle que $\overline{M} \in \ker\overline{d}$ (où $\overline{M}$ est la classe de M dans $\mathrm{PGL}_n(k)$). On a $\det M = \lambda^n$ pour $\lambda \in k^\times$ donc la matrice $N \coloneqq \lambda^{-1}M \in \mathrm{SL}_n(k)$ vérifie $\overline{N} = \overline{M}$. Par ce qui précède, l'élément $\overline{N} = \pi(N)$ est bien dans le sous-groupe de $\mathrm{PGL}_n(k)$ isomorphe à $\mathrm{PSL}_n(k)$ identifié auparavant. Réciproquement, si $N \in \mathrm{SL}_n(k)$ alors

$$\begin{aligned}\overline{d}(\overline{\pi}(N\mu_n(k)I_n)) &= \overline{d}(\overline{N}) \\ &= d(N) \\ &= 1,\end{aligned}$$

donc finalement on a bien $\ker\overline{d} = \mathrm{PSL}_n(k)$.

□

Proposition 4.3 (Automorphismes)**.** *Soit* G *un groupe. Le groupe* $\mathrm{Int}(G)$ *est distingué dans* $\mathrm{Aut}(G)$*, et le quotient est le groupe* $\mathrm{Out}(G)$ *des automorphismes* extérieurs*.*

On rappelle qu'un résultat classique est que $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$ pour tout $n \neq 6$ (et ces groupes sont isomorphes à $\mathfrak{S}_n/\mathrm{Z}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$ si de plus $n \geq 3$), et pour $n = 6$ le groupe $\mathrm{Int}(\mathfrak{S}_6)$ est d'indice 2 dans $\mathrm{Aut}(\mathfrak{S}_6)$. (En fait $\mathrm{Aut}(\mathfrak{S}_6)$ est isomorphe à un produit semi-direct (non direct) entre $\mathfrak{S}_6$ et $\mathbb{Z}/2\mathbb{Z}$.)

5 Groupes simples

Définition 5.1. Un groupe non trivial est *simple* s'il ne possède pas de sous-groupe propre strict distingué.

Les groupes finis simples sont (peut-être) classifiés, suite à de très très (très) gros travaux dans la moitié du XX$^{\text{e}}$ siècle (et ça n'est pas vraiment encore fini). Outre les $\mathbb{Z}/p\mathbb{Z}$, les deux cas importants pour nous sont les suivants.

Proposition 5.2. *Les groupes* $\mathfrak{A}_n$ *pour* $n \geq 5$ *et* $\mathrm{PSL}_n(q)$ *pour* $(n,q) \neq (2,2),(2,3)$ *sont simples.*

Remarque 5.3. Les groupes $\mathfrak{A}_n$ pour $n \in \{1,2,3\}$ sont également simples, mais sont « comptés » dans les cycliques d'ordre premier. Le groupe $\mathfrak{A}_4$ n'est quant à lui pas simple (le groupe de Klein des doubles transpositions est distingué), c'est donc le seul groupe alterné non simple.

À priori cette notion n'est pas vraiment intéressante dans le cadre de ce complément puisqu'il n'y a pas de groupe distingué ! On peut néanmoins exploiter le résultat ci-dessus.

Proposition 5.4. *Soit $n \geq 5$. Le seul groupe distingué propre non trivial de $\mathfrak{S}_n$ est $\mathfrak{A}_n$.*

Démonstration. Soit H un sous-groupe distingué de $\mathfrak{S}_n$. Alors $H \cap \mathfrak{A}_n$ est un sous-groupe distingué de $\mathfrak{A}_n$, donc $H \cap \mathfrak{A}_n = \{1\}$ ou $\mathfrak{A}_n \subseteq H$. Dans le deuxième cas on trouve $H = \mathfrak{A}_n$ ou $\mathfrak{S}_n$, on suppose donc que $H \cap \mathfrak{A}_n = \{1\}$. Mais alors la restriction de la signature à H est injective, donc H possède au plus deux éléments. On suppose que $H \neq \{1\}$ et on note σ l'unique élément non trivial de H. Puisque H est distingué dans $\mathfrak{S}_n$ on en déduit que $\sigma \in \mathrm{Z}(\mathfrak{S}_n)$, donc $\sigma = 1$ puisque $n \geq 5 \geq 3$. □

De façon analogue, on a les résultats suivant (voir par exemple P. Ortiz, *Exercices d'algèbre*, IV.15 et IV.16).

Proposition 5.5. *On suppose que $(n,k) \neq (2,\mathbb{F}_2), (2,\mathbb{F}_3)$.*
- *Les sous-groupes distingués stricts de $\mathrm{SL}_n(k)$ sont les sous-groupes du centre $\mu_n(k)I_n$.*
- *Les sous-groupes distingués stricts de $\mathrm{GL}_n(k)$ sont, pour G décrivant les sous-groupes de $k^\times$, soit de la forme GI_n soit $\det^{-1}(G) = \{M \in \mathrm{GL}_n(k) : \det(M) \in G\} \supseteq \mathrm{SL}_n(k)$.*

6 Groupe résolubles

Soit G un groupe.

Définition 6.1. On dit que G est *résoluble* s'il existe une suite de sous-groupes

$$\{1\} \triangleleft G_1 \triangleleft \cdots \triangleleft G_n \triangleleft G,$$

telle que les quotients G_{i+1}/G_i soient abéliens.

Remarque 6.2. (Largement hors programme.) Cette définition prend ses origines dans la résolution des équations polynomiales. À un polynôme on peut associer son *groupe de Galois*, qui est résoluble ssi on peut exprimer les racines du polynôme à l'aide de racines (pas forcément carrées). C'est ainsi que Galois a posé les bases de ce qui s'appelle maintenant la *théorie de Galois*.

Rappelons la définition des sous-groupes dérivées itérés (cf. Corollaire 3.13).

Proposition 6.3. *Le groupe G est résoluble ssi il existe $i \geq 0$ tel que $\mathrm{D}^i(G) = \{1\}$.*

Démonstration. On suppose que G est résoluble. Le groupe G/G_n est abélien donc par (3.12) on sait que $\mathrm{D}(G) \subseteq G_n$. De même, chaque G_{i+1}/G_i est abélien donc $\mathrm{D}(G_{i+1}) \subseteq G_i$. On trouve ainsi que $\mathrm{D}^n(G) \subseteq \mathrm{D}^{n-1}(G_n) \subseteq \mathrm{D}^{n-2}(G_{n-1}) \subseteq \cdots \subseteq \mathrm{D}(G_1) = \{1\}$.

Réciproquement, on suppose que $\mathrm{D}^m(G) = \{1\}$ pour un certain $m \geq 0$. La suite $\{1\} \triangleleft \mathrm{D}^{m-1}(G) \triangleleft \cdots \triangleleft \mathrm{D}(G) \triangleleft G$ montre que G est résoluble, puisque chaque $\mathrm{D}^{i-1}(G)/\mathrm{D}^i(G)$ est abélien par (3.12). □

Corollaire 6.4. *Si H est un sous-groupe de G et si G est résoluble alors H est résoluble.*

Démonstration. On a $\mathrm{D}^i(H) \subseteq \mathrm{D}^i(G)$ pour tout $i \geq 0$. (On peut aussi dire que $H \cap G_i \triangleleft H \cap G_{i+1}$ et qu'on a des injections $H \cap G_{i+1}/H \cap G_i \hookrightarrow G_{i+1}/G_i$.) □

La proposition suivante est très utile en pratique.

Proposition 6.5. *Le groupe G est résoluble ssi il existe $H \triangleleft G$ tel que H et G/H soient résolubles.*

Démonstration. Soit $\pi : G \twoheadrightarrow G/H$ la projection canonique. Par récurrence on a $\pi(\mathrm{D}^i(G)) \subseteq \mathrm{D}^i(G/H)$ pour tout $i \geq 0$, et on a en fait égalité puisque π est surjective. Ainsi, si G est résoluble, on vient de voir que H est également résoluble et en fait G/H aussi puisque $\mathrm{D}^i(G/H) = \pi(\mathrm{D}^i(G/H))$ donc on conclut par la Proposition 6.3.

On suppose maintenant que H et G/H sont résolubles. Par la même égalité $\pi(\mathrm{D}^i(G)) = \mathrm{D}^i(G/H)$ et la même Proposition 6.3 on en déduit que $\mathrm{D}^i(G) \subseteq H$ pour $i \gg 0$ puisque G/H est résoluble, donc $\mathrm{D}^{i+j}(G) \subseteq \mathrm{D}^j(H) = \{1\}$ pour $j \gg 0$ donc G est résoluble. □

Application 6.6. Soit B le sous-groupe des matrices triangulaires supérieures inversibles de taille n à coefficients dans un corps k. Pour chaque $m \in \{0, \dots, n-2\}$, soit U_m le sous-groupe de B constitué des matrices unitriangulaires (*i.e.* triangulaires avec des 1 sur la diagonales) avec seulement des 0 sur les m premières sur-diagonales.

Le sous-groupe U_{n-2} est isomorphe à k qui est commutatif donc résoluble. Pour $m \in \{0, \dots, n-3\}$, l'application qui à une matrice $M \in U_m$ associe le $(n-m-1)$-uplet de ses coefficients sur-diagonaux est un morphisme $U_m \to k^{n-m-1}$ surjectif et de noyau U_{m+1}. Par hypothèse de récurrence le sous-groupe U_{m+1} est résoluble, et par le premier théorème d'isomorphisme le groupe $U_m/U_{m+1} \simeq k^{n-m-1}$ également puisque k^{n-m-1} est abélien. Ainsi, par la proposition précédente on sait que U_m est résoluble.

En particulier, le groupe des matrices unitriangulaires et résoluble, et de la même façon en utilisant le morphisme $B \twoheadrightarrow U_0$ de noyau $k^{\times n}$ on montre que le sous-groupe B des matrices triangulaires supérieures inversibles est résoluble.

Il faut savoir ce qu'il en est de la résolubilité des groupes classiques. Les groupes symétriques d'indice au plus 4 sont résolubles, et à partir de l'indice 5 ils ne le sont plus (car $\mathfrak{A}_n$ est alors simple). De même, puisque SL_n est son propre groupe dérivé les groupes SL_n et GL_n ne sont pas résolubles. En revanche, par la Proposition 6.5 on sait que les p-groupes sont résolubles, en utilisant le fait que le centre d'un p-groupe n'est pas trivial.

Concluons cette section en mentionnant le fait que les groupes résolubles sont des cas particuliers des groupes *nilpotents*.

Définition 6.7. On dit que G est *nilpotent* si la suite $\left(\mathrm{C}^i(G)\right)_{i \geq 0}$ de sous-groupes de G définie par $\mathrm{C}^0(G) \coloneqq G$ et $\mathrm{C}^{i+1}(G) \coloneqq \left[\mathrm{C}^i(G), G\right]$ stationne au groupe trivial.

En particulier, on a $\mathrm{C}(G) = \mathrm{D}(G)$ donc si G est abélien alors G est nilpotent.

Proposition 6.8. *Un groupe nilpotent est résoluble.*

Démonstration. On a $\mathrm{C}^0(G) \supseteq \mathrm{D}^0(G)$ et par récurrence, si $\mathrm{C}^i(G) \supseteq \mathrm{D}^i(G)$ alors

$$\mathrm{C}^{i+1}(G) = \left[\mathrm{C}^i(G), G\right] \supseteq \left[\mathrm{D}^i(G), \mathrm{D}^i(G)\right] = \mathrm{D}^{i+1}(G).$$

□

Exemple 6.9. Le groupe $\mathfrak{S}_3$ n'est pas nilpotent (mais résoluble) : on montre que $\mathrm{C}^i(\mathfrak{S}_3) = \mathfrak{A}_3$ pour tout $i \geq 1$.